#6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
MARINET ET AL.

Serial No. **NOT YET ASSIGNED**

Filing Date: **HEREWITH**

For: **METHOD AND DEVICE FOR PROTECTING INTEGRATED CIRCUITS AGAINST PIRACY**

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Director, U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Transmitted herewith is a certified copy of the priority French Application No. 0017261.

Respectfully submitted,

PAUL J. DITMYER
Reg. No. 40,455
Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicant

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"EXPRESS MAIL" MAILING LABEL NUMBER EL 768537335 US

DATE OF DEPOSIT November 1, 2001

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231

Greg French
(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

(SIGNATURE OF PERSON MAILING PAPER OR FEE)

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 22 FEV. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04

THIS PAGE BLANK (USPTO)

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 DEC 2000
LIEU 13 INPI MARSEILLE

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0017261

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 28 DEC. 2000

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

OMNIPAT
MARCHAND André
24 Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

Vos références pour ce dossier *(facultatif)* 100117 FR

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF DE PROTECTION CONTRE LE PIRATAGE DE CIRCUITS INTEGRES

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale		STMICROELECTRONICS
Prénoms		
Forme juridique		SOCIETE ANONYME
N° SIREN		3 4 1 4 5 9 3 8 6
Code APE-NAF		3 2 1 B
Adresse	Rue	7, Avenue Galliéni
	Code postal et ville	94250 GENTILLY CEDEX
Pays		FRANCE
Nationalité		FRANCE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 DEC 2000
LIEU 13 INPI MARSEILLE

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0017261

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		100117 FR
6 MANDATAIRE		
Nom		MARCHAND
Prénom		André
Cabinet ou Société		OMNIPAT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
N° de téléphone *(facultatif)*		04.42.99.06.60.
N° de télécopie *(facultatif)*		04.42.99.06.69.
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
MARCHAND André - CPI N° 95 0303
OMNIPAT

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11 235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

28 DEC 2000
13 INPI MARSEILLE

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	100117 FR
N° D'ENREGISTREMENT NATIONAL 0017261	0017261

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
PROCEDE ET DISPOSITIF DE PROTECTION CONTRE LE PIRATAGE DE CIRCUITS INTEGRES

LE(S) DEMANDEUR(S) :
MARCHAND André
OMNIPAT
24, Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		MARINET	
Prénoms		Fabrice	
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance	
	Code postal et ville	13100	AIX EN PROVENCE
Société d'appartenance *(facultatif)*			
Nom		WUIDART	
Prénoms		Sylvie	
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance	
	Code postal et ville	13100	AIX EN PROVENCE
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)
Aix en Provence, le 28 décembre 2000
MARCHAND André - CPI N° 95 0303
OMNIPAT

PROCEDE ET DISPOSITIF DE PROTECTION CONTRE LE PIRATAGE DE CIRCUITS INTEGRES

La présente invention concerne un procédé de protection d'un circuit intégré contre le piratage, au moins lors de l'exécution par le circuit d'opérations impliquant la lecture de données confidentielles stockées dans le circuit intégré.

La présente invention concerne également un circuit intégré comprenant au moins une mémoire dans laquelle sont stockées des données confidentielles, des moyens de calcul aptes à lire les données confidentielles stockées dans la mémoire, et un dispositif de protection contre le piratage de ces données confidentielles.

De façon classique, les transactions électroniques faites sur un terminal au moyen d'une carte à puce sont sécurisées grâce à une procédure d'authentification de la carte faisant intervenir un algorithme de cryptographie. Au cours d'une telle procédure d'authentification, le terminal envoie à la carte un code aléatoire, et la carte à puce doit répondre en produisant un code d'authentification qui est la transformée du code aléatoire par l'algorithme de cryptographie. Le terminal calcule de son côté la transformée du code aléatoire et compare le résultat obtenu avec celui renvoyé par la carte. Si le code d'authentification renvoyé par la carte est valable, la transaction est autorisée.

Dans le circuit intégré d'une carte à puce, l'algorithme de cryptographie est généralement exécuté par un circuit à logique câblée, ou co-processeur de cryptographie, auquel est attribué une clé secrète ou clé de cryptographie, qui est stockée dans une zone protégée de la mémoire du circuit intégré. Il est donc essentiel de garantir une protection absolue de cette

clé secrète car les algorithmes de cryptographie mis en œuvre dans les procédures d'authentification sont en soi connus et seule la clé secrète garantit l'inviolabilité de la procédure d'authentification.

Or ces dernières années, les techniques de piratage des circuits intégrés ont considérablement évolué et mettent aujourd'hui en œuvre des méthodes d'analyse sophistiquées basées sur une observation du courant consommé par les éléments du circuit intégré lors de l'exécution d'opérations confidentielles. Il existe à ce jour deux types de méthodes d'analyse du courant consommé, à savoir les méthodes d'analyse de type SPA (Single Power Analysis) et les méthodes d'analyse de type DPA (Differential Power Analysis). Les méthodes d'analyse du type DPA, plus efficaces que les méthodes du premier type, permettent de découvrir une clé secrète par la seule observation des variations de courant consommé par le circuit de cryptographie, sans qu'il soit nécessaire de lire les données circulant sur le bus interne du circuit intégré et d'identifier les mémoires lues. Une telle méthode repose sur une corrélation d'échantillons de courant consommé avec un modèle mathématique du circuit de cryptographie et d'hypothèses sur la valeur de la clé secrète. La corrélation permet de supprimer la partie continue du courant consommé et de mettre en évidence des pics de consommation qui sont révélateurs des opérations effectuées par le circuit de cryptographie et de la valeur des données confidentielles. Avec une telle méthode, il suffit ainsi d'acquérir environ 1000 échantillons pour obtenir une clé secrète de type DES.

Pour contrer ces méthodes de piratage, on a prévu d'appliquer diverses méthodes de contre-mesure permettant de masquer ou brouiller les variations de la consommation électrique, au moins pendant l'exécution d'opérations confidentielles. De telles contre-mesures permettent uniquement d'augmenter le nombre

d'échantillons nécessaires jusqu'à 200 000, nombre qu'il est toujours possible d'obtenir moyennant une automatisation les mesures.

Dans ce contexte, la présente invention a pour but d'offrir une protection supplémentaire aux circuits intégrés conçus pour manipuler des informations confidentielles, notamment ceux équipant les cartes à puce.

Cet objectif est atteint par la prévision d'un procédé pour la protection d'un circuit intégré contre le piratage, caractérisé en ce qu'il comprend les étapes exécutées par le circuit intégré avant une séquence prédéterminée de traitements, consistant successivement à :

- détecter l'état d'au moins une temporisation,
- commander le déclenchement de la temporisation se celle-ci n'est pas active, et
- se bloquer si la temporisation est active.

Selon une particularité de l'invention, ce procédé comprend en outre une étape exécutée par le circuit intégré si la séquence de traitements prédéterminés a été exécutée normalement, consistant à désactiver la temporisation.

Selon une autre particularité de l'invention, ce procédé comprend en outre une étape exécutée par le circuit intégré si la temporisation est détectée active, consistant à modifier la valeur d'un compteur dans une zone protégée d'une mémoire non volatile, comparer la valeur de ce compteur à un seuil prédéfini, et effectuer un traitement de protection de données confidentielles stockées dans des mémoires du circuit intégré si la valeur du compteur atteint le seuil prédéfini.

Avantageusement, ledit traitement de protection consiste à effacer les données confidentielles des mémoires du circuit intégré.

Plus précisément, ledit traitement de protection consiste à effacer un code secret stocké dans une

mémoire du circuit intégré.

Alternativement, ledit traitement de protection consiste à effacer toutes mémoires du circuit intégré.

Avant d'exécuter un calcul d'une séquence d'un nombre prédéfini de calculs, le circuit intégré détecte de préférence l'état d'une temporisation respective, chaque calcul étant associé respectivement à une temporisation, il commande l'activation de la temporisation associée si celle-ci n'est pas active, et il se bloque si la temporisation associée est active.

L'invention concerne également un circuit intégré protégé contre le piratage, caractérisé en ce qu'il comprend au moins un circuit de temporisation comprenant des moyens d'activation d'une temporisation conçue pour rester à l'état actif tant que le circuit est sous tension et pendant une durée prédéterminée si le circuit est hors tension, des moyens d'inactivation de la temporisation, et des moyens pour détecter l'état actif ou inactif de la temporisation ; le circuit intégré comprenant en outre des moyens pour lire l'état de la temporisation, et pour se bloquer à des instants prédéfinis si la temporisation est à l'état actif.

Selon une particularité de l'invention, ce circuit intégré comprend en outre des moyens pour désactiver la temporisation à la suite d'une exécution normale d'une séquence de traitements prédéterminée.

Avantageusement, chaque circuit de temporisation comprend en outre des moyens pour détecter la présence de la tension d'alimentation, et des moyens pour autoriser l'activation ou l'inactivation de la temporisation lorsque la tension d'alimentation est détectée présente pendant une durée prédéterminée.

Selon une autre particularité de l'invention, ce circuit intégré comprend plusieurs circuits de temporisation, chaque circuit de temporisation étant associé à un calcul effectué par le circuit intégré, le circuit intégré comprenant des moyens pour, avant chaque

calcul, déterminer l'état de la temporisation associée au calcul, activer la temporisation associée si celle-ci n'est pas active et se bloquer si la temporisation associée est active.

De préférence, chaque circuit de temporisation comprend un condensateur associé à :

- un circuit de décharge conçu de manière à ce que le condensateur se décharge lentement lorsque le dispositif est hors tension,
- un circuit de détection de la charge du condensateur,
- des moyens de commande de la charge du condensateur, et
- des moyens de commande de la décharge du condensateur.

Avantageusement, les moyens de commande de la décharge du condensateur sont conçus pour décharger le condensateur plus rapidement que lorsque le dispositif est hors tension.

Selon encore une autre particularité de l'invention, ce circuit intégré comprend un transistor MOS présentant des courants de fuite très faibles, qui est associé au condensateur de manière à ce que celui-ci se décharge uniquement par ces courants de fuite, lorsque le circuit intégré est hors tension.

De préférence, il comprend également un circuit de test commandé par une commande de test, pour diminuer la durée de la temporisation.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés plus en détail dans la description suivante d'un mode de réalisation préféré de l'invention, faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

- la figure 1 représente schématiquement un circuit intégré selon l'invention, en liaison avec un terminal ;
- la figure 2 montre en détail un exemple de

dispositif de protection selon l'invention, équipant le circuit intégré représenté sur la figure 1 ;

- la figure 2a est un schéma détaillé d'un élément de circuit du dispositif représenté sur la figure 2 ;
- les figures 3a à 3e représentent des courbes en fonction du temps de signaux électriques illustrant le fonctionnement des circuits représentés sur les figures 2 et 2a.
- les figures 4a à 4d représentent d'autres courbes en fonction du temps de signaux électriques illustrant le fonctionnement des circuits représentés sur les figures 2 et 2a, lorsque ces circuits sont mis successivement hors tension, puis sous tension ;
- les figures 5a à 5f sont des courbes en fonction du temps de signaux électriques illustrant le fonctionnement général du circuit représenté sur la figure 2 ;
- les figures 6a à 6d représentent des courbes en fonction du temps de signaux électriques illustrant le fonctionnement général du circuit représenté sur la figure 2, en cas de remise sous tension du circuit à la suite de la détection d'un fonctionnement anormal ;
- les figures 7a à 7d représentent des courbes en fonction du temps de signaux électriques illustrant le fonctionnement général d'une variante du circuit intégré selon l'invention ;

La figure 1 représente schématiquement l'architecture classique d'un circuit intégré 1 pour carte à puce. Ce circuit intégré 1 comprend une unité centrale de traitement 2, par exemple de type microprocesseur ou microcontrôleur, une unité de liaison 7 pour pouvoir communiquer avec ou sans contact avec un terminal externe 10, un circuit de cryptographie 6 et des mémoires 4, à savoir une mémoire morte ROM dans laquelle est stocké le système d'exploitation de l'unité centrale 2, une mémoire vive RAM pour stocker des données temporaires, et une mémoire programmable et

effaçable, par exemple du type EEPROM, pour stocker un ou plusieurs programmes applicatifs. L'unité centrale 2, les mémoires 4, le circuit de cryptographie 6 et l'unité de liaison 7 sont interconnectés par un bus de données commun 3.

Une clé secrète utilisée par le circuit de cryptographie 6 est stockée dans une zone protégée de la mémoire ROM ou EEPROM.

Le circuit intégré peut également comprendre un circuit de contre-mesures 8 conçu pour brouiller une analyse de type DPA.

Selon l'invention, le circuit intégré 1 comprend également un circuit de temporisation 5 pour résister plus efficacement à une attaque de type DPA.

Sur la figure 2, ce circuit 5 comprend un circuit de temporisation, lequel comporte un transistor nMOS M1 conçu avantageusement de manière à présenter un courant de fuite drain-source très faible, c'est-à-dire un périmètre et une surface de drain minimum. Le drain de ce transistor est relié à la masse par l'intermédiaire d'un autre transistor nMOS 27 dont la grille est reliée à une entrée de commande de décharge Dchrg. Le drain du transistor M1 est également relié par l'intermédiaire d'une diode D1 montée en inverse au drain d'un transistor pMOS 24 dont la source est reliée à la source de tension V_{dd}. La grille du transistor 24 est connectée à la sortie d'un inverseur 25 dont l'entrée est connectée à la sortie d'une porte OU 23. Cette porte OU 23 présente une première entrée reliée à l'entrée de commande de chargement Chrg du circuit 5, et une seconde entrée reliée à la sortie Q du circuit 5. De cette manière, si la sortie Q ou la commande de charge Chrg est au niveau logique 1, la source du transistor est placée au niveau logique 1. Inversement, si Q et Chrg sont au niveau logique 0, le drain du transistor M1 est isolé par la diode D1 qui est alors bloquée. Cette diode est de préférence une diode de type caisson, de manière

à être isolée du substrat (c'est-à-dire de la masse) sur lequel est formé le transistor M1, pour réduire les courants de fuite.

Par ailleurs, la source du transistor M1 est reliée d'une part à la masse par l'intermédiaire d'un condensateur C, et d'autre part à la sortie Q du circuit 5 par l'intermédiaire de deux étages inverseurs montés en série permettant de transformer la tension aux bornes du condensateur C en un signal logique. D'une manière classique, chaque étage inverseur comprend un transistor pMOS 28, 30 et un transistor nMOS 29, 31, montés en série entre la source de tension V_{dd} et la masse. Les transistors 28 à 31 sont réalisés de manière à ce qu'une très faible tension aux bornes du condensateur permette d'obtenir un niveau logique 1 en sortie Q.

En outre, la grille du transistor M1 est connectée à la sortie d'une porte ET 22 dont les entrées sont respectivement connectées à un circuit 32 de détection de la tension d'alimentation V_{dd} et à la sortie d'une porte OU 21. La porte OU 21 comprend trois voies d'entrée, à savoir une première voie connectée à la sortie Q, une seconde voie reliée à l'entrée Chrg de commande de chargement, et une troisième voie reliée à la commande de déchargement Dchrg.

La figure 2a montre en détail le circuit 32 de détection de la tension d'alimentation V_{dd}. Ce circuit comprend deux transistors pMOS 35, 36 montés en diode (grille connectée au drain), ces deux transistors étant montés en série entre la source de tension V_{dd} et le drain d'un transistor nMOS 37 dont la grille est connectée à la source de tension V_{dd} et la source est connectée à la masse, afin de jouer le rôle de résistance. Le point de jonction entre les transistors 36 et 37 est connecté à un premier étage inverseur comprenant un transistor pMOS 38 dont la source est au potentiel V_{dd} et un transistor nMOS 39 dont la source est à la masse, ce point de jonction étant connecté aux

grilles des deux transistors 38 et 39. Le point de jonction entre les drains des transistors 38 et 39 est connecté à un condensateur 40 dont l'autre borne est à la masse, et à un second étage inverseur comprenant un transistor pMOS 41 dont la source est au potentiel V_{dd}, et un transistor nMOS 42 dont la source est à la masse, le point de jonction des drains des deux transistors 41, 42 fournissant le signal Enable de sortie du circuit 32. En fait, l'ensemble constitué du condensateur 40 et du dernier étage inverseur avec les transistors 41 et 42 fonctionne comme une ligne à retard.

Le fonctionnement du circuit 5 est maintenant expliqué plus en détail en référence aux figures 3 et 4 donnant en fonction du temps la forme de différents signaux du circuit intégré 1.

Comme représenté sur les figures 3a à 3e, lorsque la tension d'alimentation V_{dd} du circuit atteint la valeur $2V_{TP}$, V_{TP} étant la tension de déblocage de chaque transistor 35, 36, le signal Enable passe de l'état bas à l'état haut au bout d'un certain délai d correspondant au temps de charge du condensateur 40 (figures 3a et 3b). Inversement, lorsque la tension V_{dd} redescend en dessous de $2V_{TP}$, les transistors 35 et 36 se bloquent, faisant passer le signal Enable à l'état bas.

Pour commander la charge du condensateur C, l'unité de traitement 2 envoie une impulsion sur l'entrée de charge Chrg du circuit 5 (courbe de la figure 3c), le signal Enable étant à l'état haut. Il en résulte que la sortie de la porte OU 21 passe à l'état haut, ainsi que la sortie de la porte ET 22. Une tension est alors appliquée à la grille du transistor M1. De même, la sortie de la porte OU 23 passe à l'état haut, ce qui rend passant le transistor 24. La tension d'alimentation V_{dd} du circuit est donc appliquée au drain du transistor M1 qui est alors passant, le transistor 27 étant bloqué (commande de décharge Dchrg à 0), isolant de la masse le drain du transistor M1. Il en résulte que le

condensateur C se charge comme le montre la courbe de la figure 3d. Dès que la tension aux bornes du condensateur C devient supérieure à la tension de grille V_{TH} de déblocage du transistor 29, le transistor 28 étant bloqué, le transistor 30 se débloque, plaçant la sortie Q au niveau logique 1 (courbe de la figure 3e) qui prend alors le relais de l'impulsion de charge pour maintenir passant le transistor M1. L'impulsion de commande de charge est donc choisie suffisamment large pour que la tension aux bornes du condensateur C atteigne au moins la valeur V_{TH}.

Inversement, si l'alimentation du circuit est coupée, le signal Enable passe au niveau bas, et la sortie de la porte ET 22 passe au niveau bas, ce qui bloque le transistor M1. Le condensateur C n'est donc plus sous tension et se décharge au travers du drain du transistor M1 (courant de fuite de la diode drain-substrat du transistor). Quand le circuit n'est plus alimenté, la sortie Q suit la tension d'alimentation V_{dd} et donc tombe à 0. Tant que le temps Δt correspondant à la constante de temps du circuit de décharge du condensateur ne s'est pas écoulé, la tension aux bornes du condensateur C reste supérieure à la tension de seuil V_{TH}. Par conséquent, comme représenté sur les figures 4a à 4d, toute remise sous tension du circuit avant que le temps Δt ne se soit écoulé entraîne la mise sous tension des transistors 28 et 30, et donc la remontée de la sortie Q et une recharge automatique du condensateur C.

Dans le circuit 5, la constante de temps Δt est le temps pendant lequel le circuit intégré 1 doit être mis hors tension pour que le condensateur C soit déchargé. La valeur de Δt peut être obtenue par la formule suivante :

$$\Delta t = \frac{C\Delta V}{i} \qquad (1)$$

C étant la capacité du condensateur C, ΔV la variation de tension aux bornes du condensateur pendant

le temps Δt, et i le courant de décharge.

Si l'alimentation V_{dd} du circuit intégré est coupée, le condensateur C se décharge lentement à cause des courants de fuite très faibles qui apparaissent au travers du transistor M1. Par conséquent, même si la capacité du condensateur C est très faible, de l'ordre de quelques pF, la tension aux bornes du condensateur reste supérieure au seuil de basculement des étages inverseurs pendant la durée Δt.

Dans un composant MOS, C peut valoir 10 pF, ΔV 2 V et I 10 pA. Dans ces conditions, la constante de temps Δt vaut 2 s. Typiquement, avec la technologie MOS, la constante de temps peut atteindre 5 s.

Pour augmenter la constante de temps Δt, plusieurs condensateurs peuvent être avantageusement placés en parallèle.

Si pendant que le condensateur C est chargé, l'unité de traitement 2 envoie une impulsion sur l'entrée de décharge Dchrg, le transistor 27 devient passant, ce qui place le drain du transistor M1 à la masse et donc le condensateur C se décharge alors d'une manière quasiment instantanée, les deux transistors M1 et 27 présentant à l'état passant une faible résistance.

Pendant un très cours instant, on peut remarquer que la source de tension V_{dd} est placée directement à la masse par l'intermédiaire du transistor 27, de la diode D1 et du transistor 24. Ce conflit électrique est réglé en surdimensionnant le transistor 27 et en rendant le transistor 24 résistif (petite taille). En fait, ce conflit persiste le temps que la capacité C se décharge et fasse commuter la sortie Q.

Dès que la tension aux bornes du transistor C repasse en dessous de V_{TH}, le transistor 28 devient passant, tandis que le transistor 29 se bloque. Le transistor 30 se bloque alors à son tour, tandis que le transistor 31 se débloque, plaçant à la masse la sortie Q qui passe ainsi au niveau logique 0.

La largeur de l'impulsion de commande de décharge Dchrg doit également être plus grande que le temps de décharge du condensateur C au travers des transistors M1 et 27, jusqu'à la valeur V_{TH}. Il est à noter que la commande de décharge est appliquée à la porte OU 21 pour garantir que le condensateur C se décharge complètement. Sans cette disposition, la décharge du condensateur pourrait être stoppée dès que la tension de celui-ci repasse en dessous de la tension V_{TH}, moment à partir duquel le signal Q repasse au niveau bas, ce qui bloquerait la porte 21 et donc le transistor M1.

La figure 5a représente l'évolution de la tension V_{dd} durant une transaction établie avec le circuit intégré. Peu après la mise sous tension du circuit intégré, le signal reset sur la figure 5b passe du niveau logique 0 au niveau logique 1, ce qui déclenche un traitement d'initialisation par l'unité de traitement 2, puis une série de n calculs d'authentification, comme on peut le voir sur la figure 5c qui représente l'activité de l'unité centrale 2. A la fin de ces n calculs, s'ils conduisent à une authentification du terminal 10, l'unité centrale passe en session normale pour exécuter la transaction demandée par le terminal.

En fonctionnement normal, la sortie Q (courbe de la figure 5d) est au niveau bas à la mise sous tension du circuit. A la fin de la procédure d'initialisation, le circuit 5 est commandé à l'instant t1 par l'unité de traitement 2 qui envoie une impulsion sur l'entrée Chrg, de manière à déclencher la charge du condensateur C, et donc à faire passer la sortie Q au niveau haut, le signal Enable étant au niveau haut. Dès que la tension aux bornes du condensateur a atteint la valeur V_{TH}, la sortie Q passe au niveau haut, ce qui maintient ensuite la tension de grille et de source du transistor M1 au niveau haut. Le condensateur C reste donc chargé et le signal Q est maintenu au niveau haut.

Si les calculs d'authentification (figure 5c)

conduisent à l'authentification du terminal, l'unité centrale 2 commande la décharge du condensateur C en envoyant une impulsion sur la commande de décharge Dchrg, ce qui fait repasser la sortie Q au niveau bas à l'instant t2.

Au contraire, si au cours des calculs d'authentification, l'unité centrale 2 détecte un fonctionnement anormal révélant une tentative de piratage, elle ne commande pas le déchargement du condensateur et se bloque, par exemple dans une boucle d'attente (figures 5e, 5f).

Si ensuite on tente de réinitialiser le circuit 1 en coupant son alimentation pendant une courte durée inférieure au temps de décharge du condensateur C, l'unité centrale 2 qui exécute la procédure d'initialisation, détecte que le signal Q est encore au niveau haut, indiquant que le condensateur C n'est pas complètement déchargé et se bloque (figure 6c).

De cette manière, pour réinitialiser complètement le circuit 1, il est nécessaire d'attendre au moins pendant Δt pour pouvoir redémarrer le composant dans un état normal.

Au cours d'une analyse DPA du circuit intégré, il est donc nécessaire d'attendre que le condensateur C soit déchargé entre chaque séquence d'acquisition d'échantillons de mesure de courant, ce qui allonge considérablement la durée d'une telle analyse.

Pour supprimer totalement la possibilité d'une telle analyse, on peut prévoir qu'avant chaque blocage, l'unité centrale 2 incrémente un compteur de blocage mémorisé dans la mémoire EEPROM et se bloque définitivement lorsque la valeur du compteur atteint ou dépasse un certain seuil prédéfini. Le blocage définitif du circuit intégré peut par exemple consister à effacer la clé secrète mémorisée dans la mémoire EEPROM, ou d'une manière plus générale, à effacer toutes les données confidentielles stockées dans cette mémoire, ou

encore tout le contenu de celle-ci.

On peut prévoir par ailleurs de connecter le drain du transistor M1 à un transistor nMOS 26 dont la grille est relié à une entrée de commande de test et dont la source est reliée à un circuit 33 comprenant une pluralité de transistors nMOS en parallèle entre la source du transistor 26 et la masse, ces transistors étant montés en mode bloqué (grille reliée à la masse). Ces transistors sont de même taille que le transistor M1, de sorte que le courant de fuite qui décharge la capacité C est n fois plus important que celui de M1, n étant le nombre de transistors du circuit 33. Ce circuit 33 permet donc de rabaisser la constante de temps $\Delta t = RC$ du circuit de temporisation à une valeur compatible à la réalisation de tests sur le circuit intégré 1 (R correspondant à la résistance du circuit 33 et C étant la capacité du condensateur C).

Bien entendu, la commande de test doit être rendue suffisamment inaccessible pour ne pas être activée par des pirates éventuels.

Selon une variante de l'invention, on peut prévoir d'inclure dans le circuit intégré 1 plusieurs circuits de temporisation 5, par exemple à raison d'un circuit par séquence de calcul d'authentification. Comme représenté sur les figures 7a à 7d, au lieu de commander la charge du condensateur C durant la séquence d'initialisation effectuée par l'unité de traitement 2, chaque séquence de calcul comprend une commande de lecture de la valeur du signal Qi de sortie du circuit de temporisation 5 qui lui est associé, puis, si ce signal est au niveau bas, une commande de charge du condensateur de ce circuit, de manière à faire passer le signal Qi au niveau haut comme représenté sur les figures 7b à 7d.

De cette manière, si la même séquence de calcul est demandée deux fois durant une même phase d'authentification (sans mise hors tension du circuit 1

pendant une durée suffisante), l'unité de traitement 2 le détecte en lisant la valeur du signal Qi correspondant à la séquence de calcul, et se bloque.

REVENDICATIONS

1. Procédé pour la protection d'un circuit intégré contre le piratage, caractérisé en ce qu'il comprend les étapes exécutées par le circuit intégré avant une séquence prédéterminée de traitements, consistant successivement à :

- détecter l'état d'au moins une temporisation,
- commander le déclenchement de la temporisation se celle-ci n'est pas active, et
- se bloquer si la temporisation est active.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend en outre une étape exécutée par le circuit intégré si la séquence de traitements prédéterminés a été exécutée normalement, consistant à désactiver la temporisation.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il comprend en outre une étape exécutée par le circuit intégré si la temporisation est détectée active, consistant à modifier la valeur d'un compteur dans une zone protégée d'une mémoire non volatile, comparer la valeur de ce compteur à un seuil prédéfini, et effectuer un traitement de protection de données confidentielles stockées dans des mémoires du circuit intégré si la valeur du compteur atteint le seuil prédéfini.

4. Procédé selon la revendication 3, caractérisé en ce que ledit traitement de protection consiste à effacer les données confidentielles des mémoires du circuit intégré.

5. Procédé selon la revendication 3, caractérisé en ce que ledit traitement de protection consiste à effacer un code secret stocké dans une mémoire du circuit

intégré.

6. Procédé selon la revendication 3, caractérisé en ce que ledit traitement de protection consiste à effacer toutes mémoires du circuit intégré.

7. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que, avant d'exécuter un calcul d'une séquence d'un nombre prédéfini de calculs, le circuit intégré détecte l'état d'une temporisation respective, chaque calcul étant associé respectivement à une temporisation, il commande l'activation de la temporisation associée si celle-ci n'est pas active, et il se bloque si la temporisation associée est active.

8. Circuit intégré protégé contre le piratage, caractérisé en ce qu'il comprend au moins un circuit de temporisation comprenant des moyens d'activation d'une temporisation conçue pour rester à l'état actif tant que le circuit est sous tension et pendant une durée prédéterminée si le circuit est hors tension, des moyens d'inactivation de la temporisation, et des moyens pour détecter l'état actif ou inactif de la temporisation ; le circuit intégré comprenant en outre des moyens pour lire l'état de la temporisation, et pour se bloquer à des instants prédéfinis si la temporisation est à l'état actif.

9. Circuit intégré selon la revendication 8, caractérisé en ce qu'il comprend en outre des moyens pour désactiver la temporisation à la suite d'une exécution normale d'une séquence de traitements prédéterminée.

10. Circuit intégré selon la revendication 8 ou 9, caractérisé en ce que chaque circuit de temporisation comprend en outre des moyens pour détecter la présence

de la tension d'alimentation, et des moyens pour autoriser l'activation ou l'inactivation de la temporisation lorsque la tension d'alimentation est détectée présente pendant une durée prédéterminée.

11. Circuit intégré selon l'une quelconque des revendications 8 à 10, caractérisé en ce qu'il comprend plusieurs circuits de temporisation, chaque circuit de temporisation étant associé à un calcul effectué par le circuit intégré, le circuit intégré comprenant des moyens pour, avant chaque calcul, déterminer l'état de la temporisation associée au calcul, activer la temporisation associée si celle-ci n'est pas active et se bloquer si la temporisation associée est active.

12. Circuit intégré selon l'une quelconque des revendications 8 à 11, caractérisé en ce que chaque circuit de temporisation comprend un condensateur associé à :

- un circuit de décharge conçu de manière à ce que le condensateur se décharge lentement lorsque le dispositif est hors tension,
- un circuit de détection de la charge du condensateur,
- des moyens de commande de la charge du condensateur, et
- des moyens de commande de la décharge du condensateur.

13. Circuit intégré selon la revendication 12, caractérisé en ce que les moyens de commande de la décharge du condensateur sont conçus pour décharger le condensateur plus rapidement que lorsque le dispositif est hors tension.

14. Circuit intégré selon l'une quelconque des revendications 8 à 13, caractérisé en ce qu'il comprend

un transistor MOS présentant des courants de fuite très faibles, qui est associé au condensateur de manière à ce que celui-ci se décharge uniquement par ces courants de fuite, lorsque le circuit intégré est hors tension.

15. Circuit intégré selon l'une quelconque des revendications 8 à 14, caractérisé en ce qu'il comprend un circuit de test commandé par une commande de test, pour diminuer la durée de la temporisation.

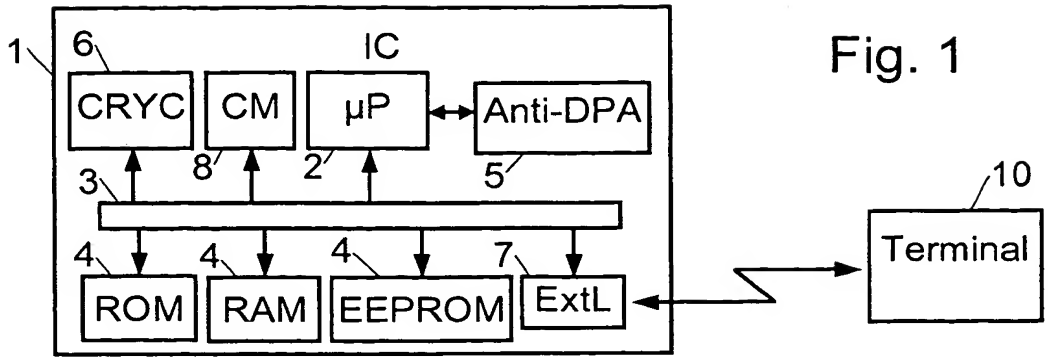

Fig. 1

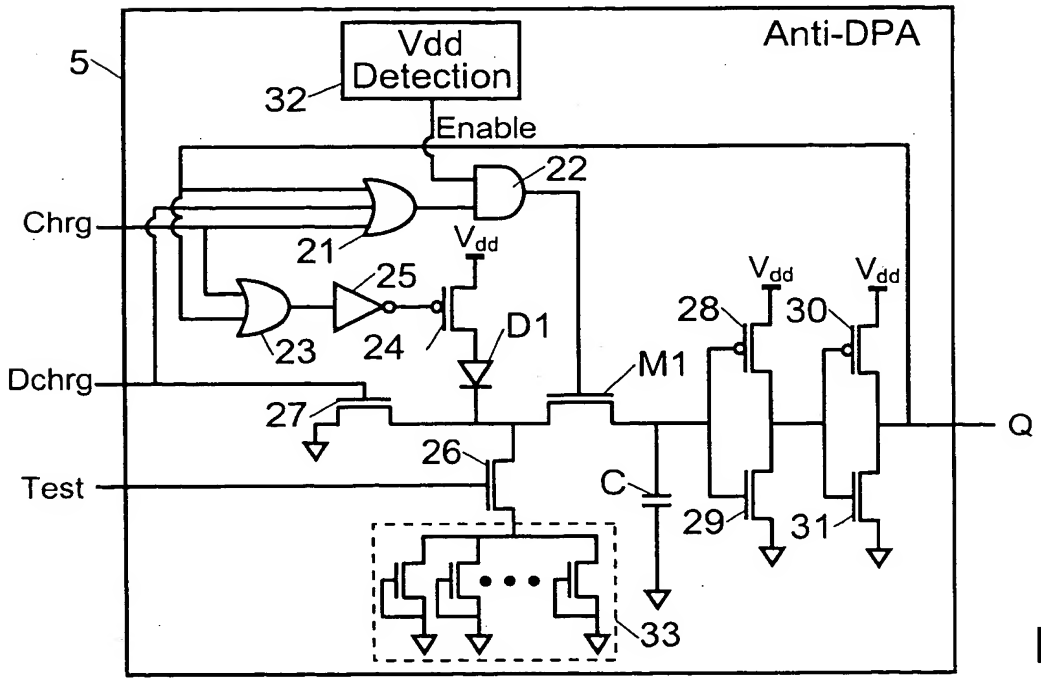

Fig. 2

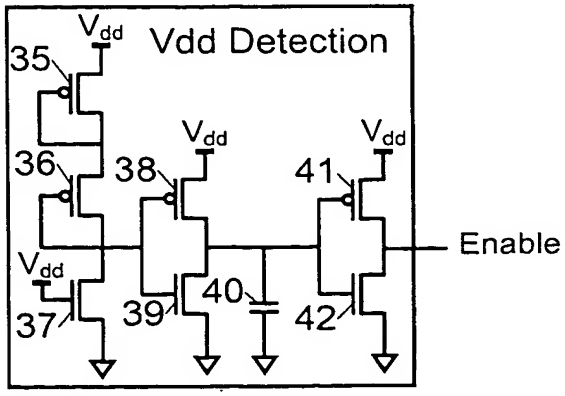

Fig. 2a

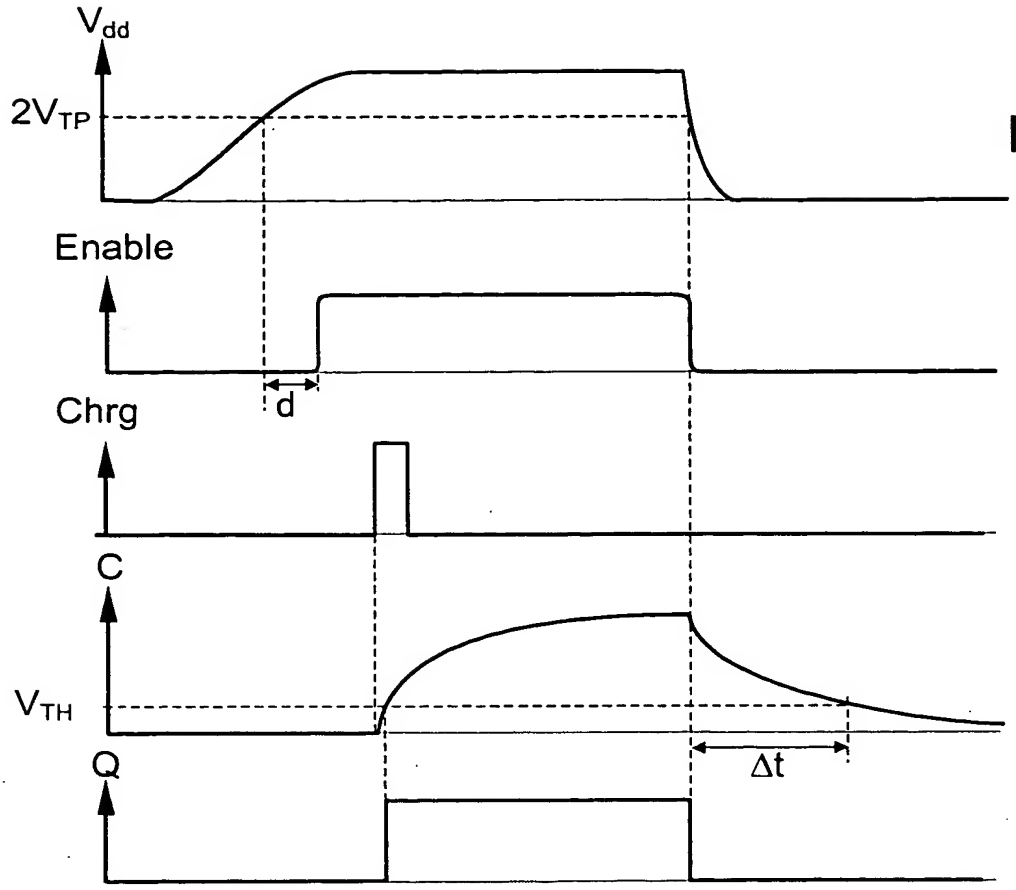

Fig. 3a

Fig. 3b

Fig. 3c

Fig. 3d

Fig. 3e

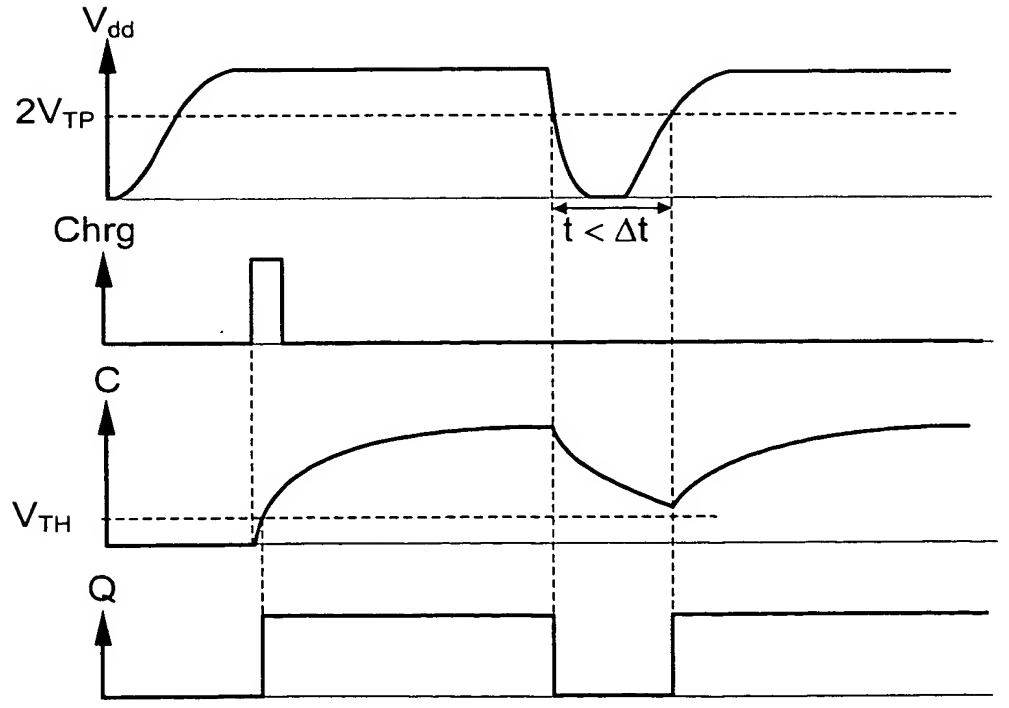

Fig. 4a

Fig. 4b

Fig. 4c

Fig. 4d

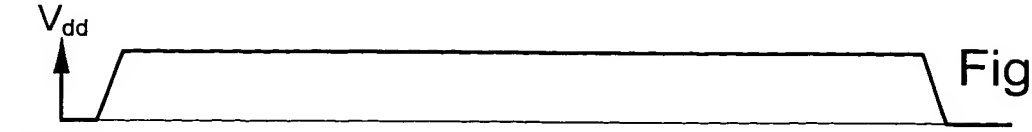

Fig. 5a

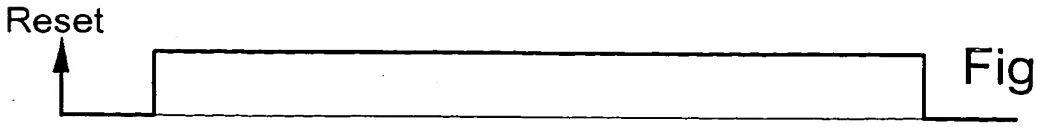

Fig. 5b

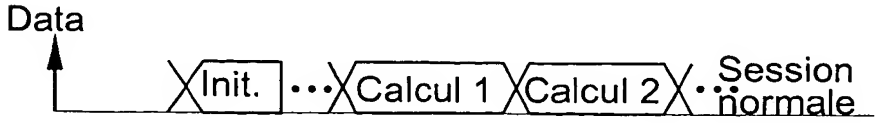

Fig. 5c

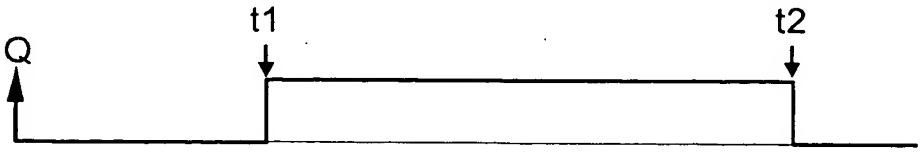

Fig. 5d

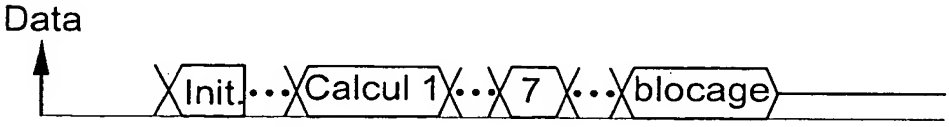

Fig. 5e

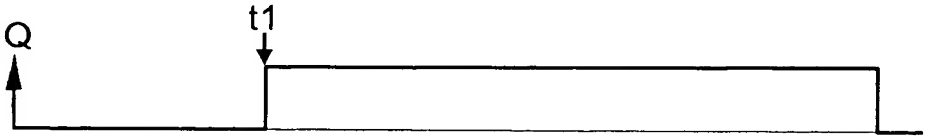

Fig. 5f

Fig. 6a

Fig. 6b

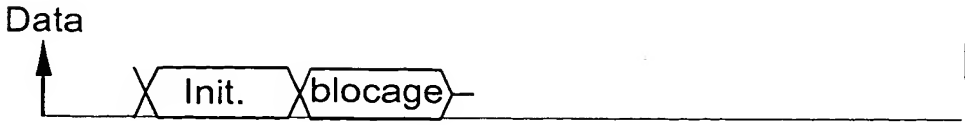

Fig. 6c

Fig. 6d

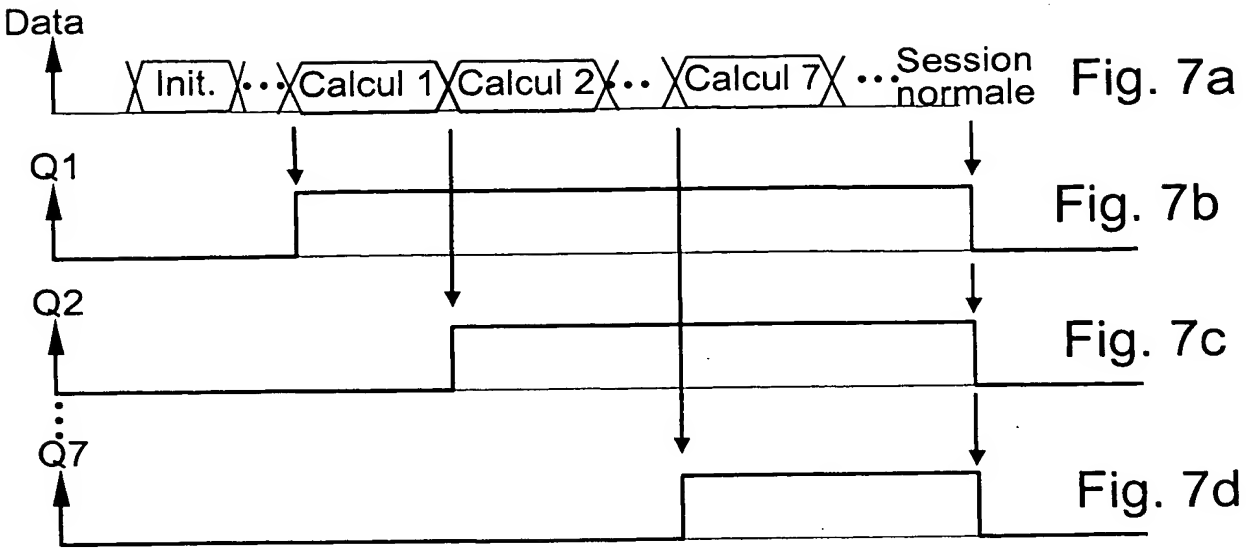

Fig. 7a

Fig. 7b

Fig. 7c

Fig. 7d